

CLAIMS

We claim:

1. A method for improving the operation of equipment used to protect a web server against attack, comprising the acts of:
 - reading a source address of a message received during an attack;
 - checking a database of privileged source addresses; and
 - instructing protective equipment for a web server to pass the received message to the web server when the source address of the received message matches an address contained in the database of privileged source addresses.
2. The method of claim 1, wherein the database of privileged source addresses includes a source address of a customer known to the web server.
3. The method of claim 1, wherein the database of privileged source addresses includes a source address of a user known to the web server.

1 4. A method for improving the operation of equipment used to protect a web server against
2 attack by a vandal, comprising the acts of:

3 reading a source address of a message received during an attack;

4 checking a database of privileged source addresses for appearance of the source address
5 of the received message;

6 when the source address of the received message appears in the database of privileged
7 source addresses, instructing protective equipment to pass the received message to a web server;

8 when the source address of the received message does not appear in the database of
9 privileged source addresses, checking a database of blocked source addresses for appearance of
10 the source address of the received message; and

11 when the source address of the received message does not appear in the database of
12 blocked source addresses, adding the source address of the received message to the database of
13 blocked source addresses and instructing the protective equipment to block the received message
14 and to block subsequent messages that bear the source address of the received message.

1 5. Protective equipment for guarding a web server against attack, comprising:

2 an address decoder for reading a source address of a message received during an attack;

3 a database of privileged source addresses; and

4 logic for instructing protective equipment for a web server to pass the message received
5 during the attack to the web server when the source address of the message received during the
6 attack matches a privileged source address contained in the database of privileged source
7 addresses.

8
9 6. The intrusion detection security system of claim 5, wherein the database of privileged source
10 addresses includes a source address of a customer known to access the web server.

11 7. The intrusion detection security system of claim 5, wherein the database of privileged source
12 addresses includes a source address of a known users of the web server.

1 8. Protective equipment for guarding a web server against attack, comprising:

2 an address decoder for reading a source address of a message received during an attack;

3 a database of privileged source addresses;

4 a database of blocked source addresses; and

5 logic for checking the database of privileged source addresses and the database of
6 blocked source addresses for appearance of the source address of the message received during the
7 attack and, responsive to the appearance, instructing protective equipment to block incoming
8 messages that bear the source address of the message received during the attack.

1 9. Protective equipment for guarding a web server against attack, comprising:

2 an address decoder for reading a source address of a message received during an attack;

3 a database of privileged source addresses;

4 a database of blocked source addresses; and

5 logic for:

6 checking the database of privileged source addresses for appearance of the source
7 address of the received message;

8 when the source address of the received message appears in the database of
9 privileged source addresses, instructing protective equipment to pass the received
10 message to a web server;

11 when the source address of the received message does not appear in the database
12 of privileged source addresses, checking the database of blocked source addresses for

13 appearance of the source address of the received message; and

14 When the source address of the received message does not appear in the database
15 of blocked source addresses, adding the source address of the received message to the
16 database of blocked source addresses and instructing the protective equipment to block
17 the received message and to block subsequent messages that bear the source address of
18 the received message.

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100
1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100	